Vendor Data Security Questionnaire

Please include this completed questionnaire along with the contract or service agreement for review. The responses will help us to more efficiently evaluate a vendor's cybersecurity environment and allow ITS to provide more accurate guidance.

Date of completion:	
Vendor Name:	
Vendor Agent:	
Service\Product name:	
Service\Product description:	
Augustana Sponsor:	
Augustana Sponsor Department:	
Data inventory list (Please attach file)	*Please attach separate files if appropriate*
Data layout\mapping\template (Please attach file)	

Vendor Data Protection Overview

		*Additional notes
Is there any type of integration or data sharing with other Augustana systems? (Y\N)		
Is Augustana providing data? (Y\N)		
Is Augustana exchanging data? (Y\N)		
Are administrative accounts provided for Augustana employees to manage vendor system? (Y\N)		
Are user accounts provided to Augustana employees or students? (Y\N)		
Does the product support multifactor authentication? (Y\N)		
Does the vendor require privileged access to Augustana data systems (Y\N)		

Data transmission

		*Additional notes
What is the data transfer method? (SFTP, API, File, Proxy account, N\A)		
What is the data encryption method during transmission? (Identify encryption method and level or N\A)		
Data transfer schedule (Daily,Weekly,Monthly,Quarterly,Annually,Custom,N\A)		

Vendor Employees

		*Additional notes
Do all vendor employees undergo criminal background checks (Y\N)		
Do all vendor employees participate in annual cyber security training (Y\N)		
Do all vendor employees participate in annual simulated phishing campaigns? (Y\N)		
Do all vendor employees utilize multi-factor authentication when accessing or processing client data, or vendor development and production environments? (Y\N)		
Are any vendor employees granted remote access to client data? (Y\N)		

Data Privacy

		*Additional notes
Does the vendor have a Data Privacy Policy? (Y\N)		
Does the vendor have a PCI compliance policy? (Y\N, N\A)		
Has the vendor experienced a cyber security breach in the last 5 years? (Y\N)		
Does the vendor have an employee specifically responsible for cyber security (Y\N)		
Does the vendor provide a remote work environment for employees using personal devices? (Y\N)		
Does the vendor maintain data access logs and auditing? (Y\N)		

General Business Practices

		*Additional notes
Does the vendor undergo annual penetration tests performed by a 3rd party? (Y\N)		
Does the vendor have current Higher Education customers? (Y\N)		
Does the vendor carry cybersecurity insurance? (Y\N)		
Does the vendor have a disaster recovery plan? (Y\N)		
Does the vendor have a business continuity plan? (Y\N)		
Does the vendor rely on 3rd party vendors or partners in delivering service to clients? (Y\N)		
Does the vendor require 3rd party vendors to maintain a business environment at least as secure as its own? (Y\N)		

Vendor's Business Environment

		*Additional notes
If cloud hosted, does the vendor utilize a multi-tenant environment? (Y\N, N\A)		
Is multifactor authentication required to access vendor's business environment? (Y\N)		
Does the vendor use automated intrusion detection monitoring? (Y\N)		
Does the vendor have a data backup strategy including offline or "air-gapped" backups? (Y\N)		
Does the vendor have a network firewall? (Y\N)		
Does the vendor use endpoint device protection? (Y\N)		
Does the vendor encrypt data at rest? (Y\N)		
Does the vendor encrypt data in transit? (Y\N, N\A)		